



(11)

EP 3 007 365 A1

(12)

EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:

13.04.2016 Bulletin 2016/15

(51) Int Cl.:

H04B 5/02 (2006.01)

G06Q 20/16 (2012.01)

G06Q 40/04 (2012.01)

(21) Application number: **14807406.5**

(86) International application number:

PCT/CN2014/079145

(22) Date of filing: **04.06.2014**

(87) International publication number:

WO 2014/194822 (11.12.2014 Gazette 2014/50)

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

Designated Extension States:

BA ME

• **XU, Yanjun**

Shanghai 200135 (CN)

• **LI, Wei**

Shanghai 200135 (CN)

• **LI, Jie**

Shanghai 200135 (CN)

• **WU, Shuijiong**

Shanghai 200135 (CN)

(30) Priority: **06.06.2013 CN 201310222492**

(71) Applicant: **China Unionpay Co., Ltd**

Shanghai 200135 (CN)

(74) Representative: **Berkenbrink, Kai-Oliver**

Patentanwälte Becker & Müller

Turmstrasse 22

40878 Ratingen (DE)

(72) Inventors:

• **CHAI, Hongfeng**

Shanghai 200135 (CN)

(54) **SECURE INFORMATION INTERACTION METHOD FOR ELECTRONIC RESOURCES TRANSFER**

(57) The invention proposes a security information interaction method. In the method, a first security information interaction terminal executes a security information interaction procedure based on a direct data communication with a second security information interaction terminal in the form of near field communication so as to realize the transfer of electronic resources. The security information interaction method disclosed by the invention can achieve a direct transfer of electronic resources between security information interaction terminals and has a high safety and reliability.

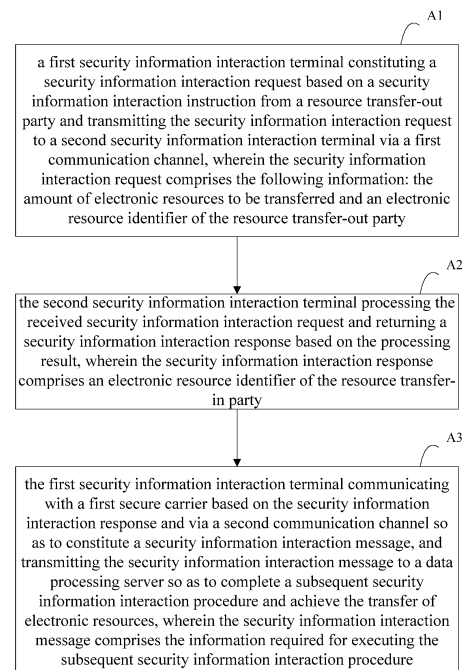


FIG. 1

EP 3 007 365 A1

Description

FIELD OF THE INVENTION

[0001] The invention relates to information interaction method, and in particular, to a security information interaction method for electronic resource transfer.

BACKGROUND

[0002] Currently, with the increasing development of network application (especially the mobile network) and increasing abundance of business types in different fields, the interaction of security information (i.e., the information that is highly demanding on security) related to transfer of electronic resource is becoming more and more important.

[0003] Existing security information interaction methods related to transfer of electronic resource are typically used only for security information interaction in a form of field offline (e.g., applying electronic cash in a form of field offline by means of financial mechanisms), and thus are difficult to achieve a direct transfer of electronic resource between security information interaction terminals (e.g., mobile terminals).

[0004] Therefore, there exists a need for a security information interaction method that can achieve a direct transfer of electronic resource between security information interaction terminals and has a high safety and reliability.

SUMMARY OF THE INVENTION

[0005] In order to address the existing problems in the above prior art solutions, the invention proposes a security information interaction method that can achieve a direct transfer of electronic resource between security information interaction terminals and has a high safety and reliability.

[0006] The object of the invention is achieved by the following technical solutions:

a security information interaction method including the following steps:

(A1) a first security information interaction terminal constituting a security information interaction request based on a security information interaction instruction from a resource transfer-out party and transmitting the security information interaction request to a second security information interaction terminal via a first communication channel, wherein the security information interaction request comprises the following information: the amount of the electronic resources to be transferred and an electronic resource identifier of the resource transfer-out party;

(A2) the second security information interaction terminal processing the received security information interaction request and returning a security information interaction response based on the processing result, wherein the security information interaction response comprises an electronic resource identifier of the resource transfer-in party;

(A3) the first security information interaction terminal communicating with a first secure carrier based on the security information interaction response and via a second communication channel so as to constitute a security information interaction message, and transmitting the security information interaction message to a data processing server so as to complete the subsequent security information interaction procedure and achieve the transfer of electronic resources, wherein the security information interaction message comprises the information required for executing the subsequent security information interaction procedure.

[0007] Preferably, in the above described technical solutions, the first communication channel is a communication channel based on near field communication protocol.

[0008] Preferably, in the above described technical solutions, the first security information interaction terminal acquires the information required for executing the subsequent security information interaction procedure from the first secure carrier via the second communication channel.

[0009] Preferably, in the above described technical solutions, the first security information interaction terminal and the second security information interaction terminal are both mobile terminals.

[0010] Preferably, in the above described technical solutions, the step (A3) further includes: the data processing server analyzing the received security information interaction message and executing an offline verification and determination operation; if the result of the offline verification and determination operation is "approving the transfer of electronic resources to be executed", an approval response is returned to the first security information interaction terminal; otherwise, a rejection response is returned to the first security information interaction terminal.

[0011] Preferably, in the above described technical solutions, the step (A3) further includes: if the approval response is received, the first security information interaction terminal conducts data communication with the first security carrier via the second communication channel so as to execute an operation related to the transfer-out of electronic resources in an offline manner and acquire a corresponding security information interaction certificate, and if a rejection response is received, the first se-

curity information interaction terminal terminates the security information interaction procedure and informs the user of the failure of security information interaction.

[0012] Preferably, in the above described technical solutions, the step (A3) further includes: after the operation related to transfer-out of electronic resources is executed, the first security information interaction terminal transmits a transfer-out operation success response to the data processing server, wherein the transfer-out operation success response comprises the security information interaction certificate and the electronic resource identifier of the resource transfer-in party.

[0013] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the transfer-out operation success response, the data processing server records the information related to current security information interaction and sets the status of this record to be "unfinished", and sends a security information interaction response to a first service provider server, wherein the security information interaction response comprises the information related to current security information interaction, and the data processing server then sends a resource transfer-in notification to the second security information interaction terminal.

[0014] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the resource transfer-in notification, the second security information interaction terminal sends a security information interaction record enquiry/synchronization request to the data processing server so as to acquire the security information interaction record whose status is "unfinished".

[0015] Preferably, in the above described technical solutions, the step (A3) further includes: after acquiring the security information interaction record whose status is "unfinished", the second security information interaction terminal sends a secure carrier electronic resource synchronization request to the data processing server for the security information interaction record whose status is "unfinished", wherein the secure carrier electronic resource synchronization request at least comprises the electronic resource identifier of the resource transfer-in party.

[0016] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the secure carrier electronic resource synchronization request, the data processing server sends a secure carrier electronic resource synchronization response to the second security information interaction terminal, wherein the secure carrier electronic resource synchronization response comprises the amount value of electronic resources to be transferred-in with a tamper-proofing protection.

[0017] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the secure carrier electronic resource synchronization response, the second tamper information interaction terminal conducts data communication with a second se-

cure carrier via a third communication channel so as to acquire the information related to electronic resource transfer-in, and then sends the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection to the data processing server.

[0018] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, the data processing server constitutes an electronic resource transfer-in request message based on the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, and sends the electronic resource transfer-in request message to a second service provider server.

[0019] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the electronic resource transfer-in request message, the second service provider server executes a determination operation based on the electronic resource transfer-in request message; if the result of the determination operation is "approving the transfer of electronic resources to be executed", an electronic resource balance value is extracted from the information related to electronic resource transfer-in, a new electronic resource balance value is calculated from the electronic resource balance value and the amount value of the electronic resources to be transferred-in, an updated script of the electronic resource balance value is generated based on the new electronic resource balance value, and then the updated script of the electronic resource balance value is sent to the data processing server.

[0020] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the updated script of the electronic resource balance value, the data processing server forwards it to the second security information interaction terminal; after receiving the updated script of the electronic resource balance value, the second security information interaction terminal forwards it to the second secure carrier; and after receiving the updated script of the electronic resource balance value, the second secure carrier executes the updated script of the electronic resource balance value so as to update the electronic resource balance value, and sends the result of script execution back to the second security information interaction terminal.

[0021] Preferably, in the above described technical solutions, the step (A3) further includes: after receiving the result of script execution, the second security information interaction terminal forwards it to the data processing server; after receiving the result of script execution, the data processing server forwards it to the second service provider server, and sends an electronic resource transfer success notification to the first security information interaction terminal.

[0022] Preferably, in the above described technical solutions, the data processing server calculates a verification code for the amount of electronic resources to be transferred, and combines the verification code and a plain text of the amount of electronic resources to be transferred together so as to form the amount value of electronic resources to be transferred-in with a tamper-proofing protection.

[0023] The security information interaction method disclosed by the invention has the following advantages: (1) a direct transfer operation of electronic resources can be executed between security information interaction terminals (especially mobile terminals); and (2) a high safety and a high reliability are ensured.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The technical features and advantages of the invention will be better understood by those skilled in the art with reference to the drawings, in which:

Fig. 1 is a flowchart of the security information interaction method according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE UTILITY MODEL

[0025] Fig. 1 is a flowchart of the security information interaction method according to an embodiment of the invention. As show in Fig. 1, the security information interaction method disclosed by the invention includes the following steps: (A1) a first security information interaction terminal constituting a security information interaction request based on a security information interaction instruction from a resource transfer-out party (e.g., a payer in a payment transaction) and transmitting the security information interaction request to a second security information interaction terminal via a first communication channel, wherein the security information interaction request comprises the following information: the amount of electronic resources to be transferred (e.g., currency amount of a transaction) and an electronic resource identifier of the resource transfer-out party (e.g., an electronic cash account of the payer party); (A2) the second security information interaction terminal processing the received security information interaction request and returning a security information interaction response based on the processing result, wherein the security information interaction response comprises an electronic resource identifier of the resource transfer-in party (e.g., an electronic cash account of the payee party); (A3) the first security information interaction terminal communicating with a first secure carrier (i.e., an carrier that can store and run a secure application for executing security information interaction procedure, e.g., SIM card, smart SD card, etc.) based on the security information interaction response and via a second communication channel so as to constitute a security information interaction message,

and transmitting the security information interaction message to a data processing server (e.g., a payment platform in financial field) so as to complete a subsequent security information interaction procedure and achieve the transfer of electronic resources, wherein the security information interaction message comprises the information required for executing the subsequent security information interaction procedure (e.g., electronic cash application data in the first secure carrier).

[0026] Preferably, in the security information interaction method disclosed by the invention, the first communication channel is a communication channel based on near field communication protocol (e.g., NFC protocol).

[0027] Preferably, in the security information interaction method disclosed by the invention, the first security information interaction terminal acquires the information required for executing the subsequent security information interaction procedure (e.g., electronic cash application data in the first secure carrier) from the first secure carrier (i.e., a secure carrier of the resource transfer-out party) via the second communication channel.

[0028] By way of example, in the security information interaction method disclosed by the invention, the first security information interaction terminal and the second security information interaction terminal are both mobile terminals (e.g., cell-phone).

[0029] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: the data processing server analyzing the received security information interaction message and executing an offline verification and determination operation; if the result of the offline verification and determination operation is "approving the transfer of electronic resources to be executed", an approval response is returned to the first security information interaction terminal; otherwise, a rejection response is returned to the first security information interaction terminal.

[0030] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: if the approval response is received, the first security information interaction terminal conducts data communication with the first secure carrier via the second communication channel so as to execute the operation related to the transfer-out of electronic resources in an offline manner (e.g., offline payment cut) and acquire a corresponding security information interaction certificate; and if a rejection response is received, the first security information interaction terminal terminates the security information interaction procedure and informs the user of the failure of security information interaction.

[0031] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after the operation related to the transfer-out of electronic resources is executed, the first security information interaction terminal transmits a transfer-out operation success response to the data processing server, wherein the transfer-out operation success response

comprises the security information interaction certificate and the electronic resource identifier of the resource transfer-in party (e.g., the electronic cash account of the payee party)

[0032] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the transfer-out operation success response, the data processing server records the information related to current security information interaction (e.g., current transaction information) and sets the status of this record to be "unfinished", and sends a security information interaction response to a first service provider server (e.g., an issuing bank of the payer party's card), wherein the security information interaction response comprises the information related to current security information interaction (e.g., current transaction information), and the data processing server then sends a resource transfer-in notification to the second security information interaction terminal (e.g., sending an account transfer-in notification in the form of short message).

[0033] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the resource transfer-in notification, the second security information interaction terminal sends a security information interaction record enquire/synchronization request to the data processing server so as to acquire the security information interaction record whose status is "unfinished".

[0034] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after acquiring the security information interaction record whose status is "unfinished", the second security information interaction terminal sends a secure carrier electronic resource synchronization request (e.g., an electronic cash balance synchronization transaction request from a smart card) to the data processing server for the security information interaction record whose status is "unfinished", wherein the secure carrier electronic resource synchronization request at least comprises the electronic resource identifier of the resource transfer-in party.

[0035] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the secure carrier electronic resource synchronization request, the data processing server sends a secure carrier electronic resource synchronization response to the second security information interaction terminal, wherein the secure carrier electronic resource synchronization response comprises the amount value of electronic resources to be transferred-in with a tamper-proofing protection (e.g., transferred-in amount information).

[0036] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the secure carrier electronic resource synchronization response, the second security information interaction terminal conducts data communication with a second secure carrier (i.e., a secure carrier

of the resource transfer-in party) via a third communication channel so as to acquire the information related to electronic resource transfer-in (e.g., electronic cash application data and balance in the second secure carrier), and then sends the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection to the data processing server.

[0037] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, the data processing server constitutes an electronic resource transfer-in request message based on the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, and sends the electronic resource transfer-in request message to a second service provider server (e.g., an issuing bank of the payee party' card).

[0038] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the electronic resource transfer-in request message, the second service provider server executes a determination operation based on the electronic resource transfer-in request message; and if the result of the determination operation is "approving the transfer of electronic resources to be executed", an electronic resource balance value (e.g., electronic cash balance) is extracted from the information related to electronic resource transfer-in, and then a new electronic resource balance value (which is the sum of the electronic resource balance value and the amount value of electronic resources to be transferred-in, e.g., a new electronic cash balance) is calculated from the electronic resource balance value and the amount value of electronic resources to be transferred-in, and an updated script of the electronic resource balance value is generated based on the new electronic resource balance value, and the updated script of the electronic resource balance value is sent to the data processing server.

[0039] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the updated script of the electronic resource balance value, the data processing server forwards it to the second security information interaction terminal; after receiving the updated script of the electronic resource balance value, the second security information interaction terminal forwards it to the second secure carrier; and after receiving the updated script of the electronic resource balance value, the second secure carrier executes the updated script of the electronic resource balance value so as to update the electronic resource balance value (that is, using the new electronic resource balance value as the current effective electronic resource balance value), and sends the result of script execution back to the second security information inter-

action terminal.

[0040] Preferably, in the security information interaction method disclosed by the invention, the step (A3) further includes: after receiving the result of script execution, the second security information interaction terminal forwards it to the data processing server; after receiving the result of script execution, the data processing server forwards it to the second service provider server, and sends an electronic resource transfer success notification to the first security information interaction terminal (e.g., sending a transaction success result notification in the form of short message).

[0041] Preferably, in the security information interaction method disclosed by the invention, the data processing server calculates a verification code for the amount of the electronic resources to be transferred, and combines the verification code and a plain text of the amount of electronic resources to be transferred together so as to form the amount value of electronic resources to be transferred-in with a tamper-proofing protection.

[0042] As can be seen from the above, the security information interaction method disclosed by the invention has the following advantages: (1) a direct transfer operation of electronic resources can be executed between security information interaction terminals (especially mobile terminals); and (2) a high safety and a high reliability are ensured.

[0043] While the invention has been described through the above preferred embodiments, the ways of implementing the same are not limited to the above embodiments. It will be appreciated that various modification and variations can be made to the invention by those skilled in the art without departing from the spirit and scope of the invention.

Claims

1. A security information interaction method, including the following steps:

(A1) a first security information interaction terminal constituting a security information interaction request based on a security information interaction instruction from a resource transfer-out party and transmitting the security information interaction request to a second security information interaction terminal via a first communication channel, wherein the security information interaction request comprises the following information: the amount of electronic resources to be transferred and an electronic resource identifier of the resource transfer-out party;

(A2) the second security information interaction terminal processing the received security information interaction request and returning a security information interaction response based on the processing result, wherein the security information

interaction response comprises an electronic resource identifier of the resource transfer-in party;

(A3) the first security information interaction terminal communicating with a first secure carrier based on the security information interaction response and via a second communication channel so as to constitute a security information interaction message, and transmitting the security information interaction message to a data processing server so as to complete a subsequent security information interaction procedure and achieve the transfer of electronic resources, wherein the security information interaction message comprises the information required for executing the subsequent security information interaction procedure.

2. A method according to claim 1, **characterized in that** the first communication channel is a communication channel based on near field communication protocol.
3. A method according to claim 2, **characterized in that** the first security information interaction terminal acquires the information required for executing the subsequent security information interaction procedure from the first secure carrier via the second communication channel.
4. A method according to claim 3, **characterized in that** the first security information interaction terminal and the second security information interaction terminal are both mobile terminals.
5. A method according to claim 4, **characterized in that** the step (A3) further includes: the data processing server analyzing the received security information interaction message and executing an offline verification and determination operation; if the result of the offline verification and determination operation is "approving the transfer of electronic resources to be executed", an approval response is returned to the first security information interaction terminal; otherwise, a rejection response is returned to the first security information interaction terminal.
6. A method according to claim 5, **characterized in that** the step (A3) further includes: if the approval response is received, the first security information interaction terminal conducts data communication with the first secure carrier via the second communication channel so as to execute the operation related to transfer-out of electronic resources in an offline manner and acquire a corresponding security information interaction certificate; and if a rejection response is received, the first security information interaction terminal terminates the security information

tion interaction procedure and informs the user of the failure of security information interaction.

7. A method according to claim 6, **characterized in that** the step (A3) further includes: after the operation related to transfer-out of electronic resources is executed, the first security information interaction terminal transmits a transfer-out operation success response to the data processing server, wherein the transfer-out operation success response comprises the security information interaction certificate and the electronic resource identifier of the resource transfer-in party. 5
8. A method according to claim 7, **characterized in that** the step (A3) further includes: after receiving the transfer-out operation success response, the data processing server records the information related to current security information interaction and sets the status of this record to be "unfinished", and sends a security information interaction response to a first service provider server, wherein the security information interaction response comprises the information related to current security information interaction, and the data processing server then sends a resource transfer-in notification to the second security information interaction terminal. 10 15 20 25
9. A method according to claim 8, **characterized in that** the step (A3) further includes: after receiving the resource transfer-in notification, the second security information interaction terminal sends a security information interaction record enquiry/synchronization request to the data processing server so as to acquire the security information interaction record whose status is "unfinished". 30 35
10. A method according to claim 9, **characterized in that** the step (A3) further includes: after acquiring the security information interaction record whose status is "unfinished", the second security information interaction terminal sends a secure carrier electronic resource synchronization request to the data processing server for the security information interaction record whose status is "unfinished", wherein the secure carrier electronic resource synchronization request at least comprises electronic resource identifier of the resource transfer-in party. 40 45
11. A method according to claim 10, **characterized in that** the step (A3) further includes: after receiving the secure carrier electronic resource synchronization request, the data processing server sends a secure carrier electronic resource synchronization response to the second security information interaction terminal, wherein the secure carrier electronic resource synchronization response comprises the amount value of electronic resources to be trans- 50 55

ferred-in with a tamper-proofing protection.

12. A method according to claim 11, **characterized in that** the step (A3) further includes: after receiving the secure carrier electronic resource synchronization response, the second security information interaction terminal conducts data communication with a second secure carrier via a third communication channel so as to acquire the information related to electronic resource transfer-in, and then sends the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection to the data processing server.
13. A method according to claim 12, **characterized in that** the step (A3) further includes: after receiving the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, the data processing server constitute an electronic resource transfer-in request message based on the information related to electronic resource transfer-in and the amount value of electronic resources to be transferred-in with a tamper-proofing protection, and sends the electronic resource transfer-in request message to a second service provider server.
14. A method according to claim 13, **characterized in that** the step (A3) further includes: after receiving the electronic resource transfer-in request message, the second service provider server executes a determination operation based on the electronic resource transfer-in request message; and if the result of the determination operation is "approving the transfer of electronic resources to be executed", an electronic resource balance value is extracted from the information related to electronic resource transfer-in, and then a new electronic resource balance value is calculated from the electronic resource balance value and the amount value of electronic resources to be transferred-in, and an updated script of the electronic resource balance value is generated based on the new electronic resource balance value, and then the updated script of the electronic resource balance value is sent to the data processing server.
15. A method according to claim 14, **characterized in that** the step (A3) further includes: after receiving the updated script of the electronic resource balance value, the data processing server forwards it to the second security information interaction terminal; after receiving the updated script of the electronic resource balance value, the second security information interaction terminal forwards it to the second secure carrier; and after receiving the updated script of the electronic resource balance value, the second

secure carrier executes the updated script of the electronic resource balance value so as to update the electronic resource balance value, and sends the result of script execution back to the second security information interaction terminal.

5

16. A method according to claim 15, **characterized in that** the step (A3) further includes: after receiving the result of script execution, the second security information interaction terminal forwards it to the data processing server; after receiving the result of script execution, the data processing server forwards it to the second service provider server, and sends an electronic resource transfer success notification to the first security information interaction terminal.
17. A method according to claim 16, **characterized in that** the data processing server calculates a verification code for the amount of electronic resources to be transferred, and combines the verification code and the plain text of the amount of electronic resources to be transferred together so as to form the amount value of electronic resources to be transferred-in with a tamper-proofing protection.

10

15

20

25

30

35

40

45

50

55

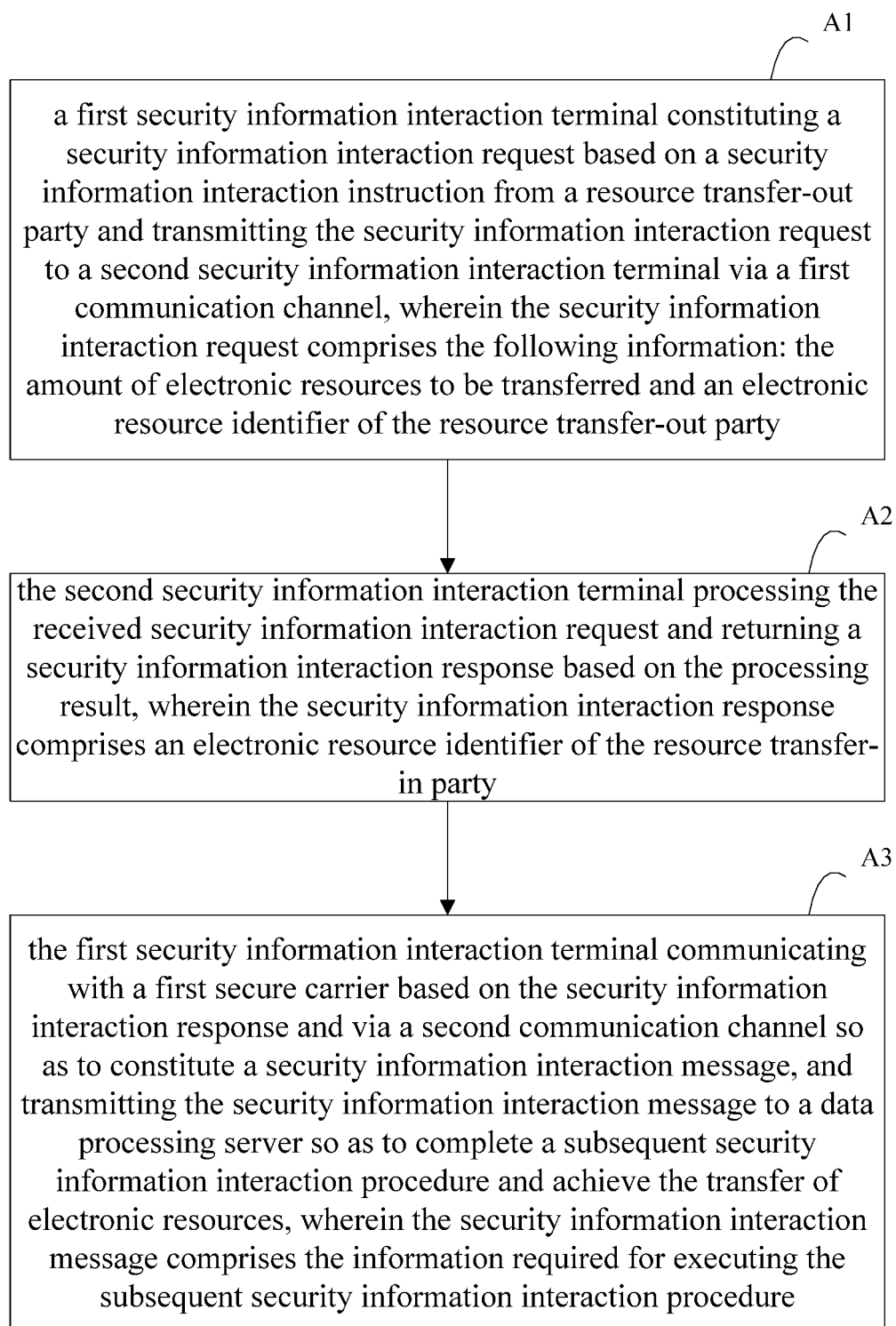


FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/079145

A. CLASSIFICATION OF SUBJECT MATTER

H04B 5/02 (2006.01) i; G06Q 20/16 (2012.01) i; G06Q 40/04 (2012.01) i
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04B; H04W; H04L; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS, CNKI, CNABS, DWPI: NFC, near field communication, terminal, mobile, transaction, payment, secure, safety, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101933246 A (EBAY INC.) 29 December 2010 (29.12.2010) see claim 1, description, paragraph [0065] and figure 6	1-4
A	CN 101933246 A (EBAY INC.) 29 December 2010 (29.12.2010) see the whole document	5-17
A	CN 102496125 A (CHENGDU INLEE TECHNOLOGY CO LTD) 13 June 2012 (13.06.2012) see the whole document	1-17
A	CN 102685692 A (ZTE CORP.) 19 September 2012 (19.09.2012) see the whole document	1-17
A	CN 102404025 A (CHENGDU INLEE TECHNOLOGY CO LTD) 04 April 2012 (04.04.2012) see the whole document	1-17

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search
04 September 2014

Date of mailing of the international search report
23 September 2014

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
CHEN, Ruyan
Telephone No. (86-10) 62411863

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/079145

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101933246 A	29.12.2010	KR 20100117639 A	03.11.2010
		WO 2009097215 A9	22.10.2009
		WO 2009097215 A1	06.08.2009
		US 8233841 B2	31.07.2012
		US 2009191811 A1	30.07.2009
CN 102496125 A	13.06.2012	None	
CN 102685692 A	19.09.2012	None	
CN 102404025 A	04.04.2012	WO 2013071711 A1	23.05.2013